INCIDENT RESPONSE FOR IN-HOUSE SOC ANALYST WITH SCENARIOS AND SIMULATIONS

BY IZZMIER IZZUDDIN

SCENARIO 1: RANSOMWARE ATTACK ON INTERNAL NETWORK

On a typical Monday morning, you receive alerts from the Endpoint Detection and Response (EDR) system indicating unusual file encryption activities on several machines in the network.

Incident Response Steps

Step 1: Identification

Alerts:

- Multiple alerts from EDR for suspicious file modifications and encryption activities.
- High CPU usage and unauthorized process creation detected on several endpoints.
- Users report being unable to access their files, with ransom notes appearing on their screens.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the ransomware.
- Identify the affected systems using logs from EDR, SIEM, and other monitoring tools.
- Note: The ransomware strain identified is "Ryuk," known for encrypting files and demanding ransom payments in Bitcoin.

System Logs from Infected Machine (Host: WORKSTATION-01)

1. EDR Alert Logs:

2024-07-23 08:15:32 [ALERT] Suspicious file modification detected - C:\Users\Izzmier\Documents\file1.docx -> C:\Users\Izzmier\Documents\file1.docx.ryuk
2024-07-23 08:15:45 [ALERT] High CPU usage by process - C:\Windows\System32\svchost.exe
2024-07-23 08:16:02 [ALERT] Unauthorized process creation detected - C:\Users\Izzmier\AppData\Local\Temp\ryuk.exe

2. Windows Event Logs:

2024-07-23 08:14:58 [Event ID 4624] Successful logon - User: Izzmier, Logon Type: 2
2024-07-23 08:15:20 [Event ID 4688] A new process has been created - New Process Name: C:\Users\Izzmier\AppData\Local\Temp\ryuk.exe
2024-07-23 08:15:22 [Event ID 5140] A network share object was accessed - Share Path: \\WORKSTATION-01\C$\Users\Izzmier\Documents

2024-07-23 08:15:32 [Event ID 4663] An attempt was made to access an object - Object Name: C:\Users\Izzmier\Documents\file1.docx

3. Firewall Logs:

2024-07-23 08:15:35 [ALERT] Outbound connection attempt blocked - Destination IP: 198.51.100.25, Port: 443
2024-07-23 08:16:00 [ALERT] Multiple outbound connection attempts - Destination IP: 198.51.100.25, Port: 443

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the affected machines from the network to prevent further spread.
  - Use network segmentation to isolate critical systems from those that are potentially compromised.
  - Disable any remote access (e.g., RDP, VPN) to the affected machines.
- **Blocking:**
  - Block known malicious IP addresses, domains, and URLs associated with Ryuk ransomware.
  - Implement temporary blocks on file-sharing protocols (e.g., SMB) to contain the spread.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, and legal teams, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., not to power off their machines).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the EDR alerts and event logs to identify infected systems (e.g., WORKSTATION-01).
   - Verify the extent of the infection using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the infected machines from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the devices.

```
# Example command to disable network interface on Windows
netsh interface set interface "Ethernet" admin=disable
```

- **Endpoint Isolation:**
  - Use EDR or remote management tools to isolate the infected endpoints.

```
# Example using an EDR platform command
edr isolate-endpoint --hostname WORKSTATION-01
```

Blocking Steps:

1. **Block Malicious IP Addresses:**
   - Use firewall rules to block outbound connections to known malicious IP addresses.

```
# Example command to block an IP address using Windows Firewall
netsh advfirewall firewall add rule name="Block Ryuk IP" dir=out action=block remoteip=198.51.100.25
```

2. **Block Malicious Domains and URLs:**
   - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the ransomware.

```
# Example using a DNS filtering solution
dns-filter add --domain "malicious-domain.com" --action block
```

3. **Restrict File Sharing Protocols:**
   - Disable or limit access to file-sharing protocols (e.g., SMB) on the affected network segments.

```
# Example command to disable SMB on Windows
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4. **Monitor and Verify:**
   - Continuously monitor network traffic and logs to ensure no further malicious activities.
   - Verify that all blocks and isolation measures are effectively preventing the spread of the ransomware.

Step 3: Eradication

Eradication Actions:

- Remove the malicious files and processes identified on the infected systems.
  - Use antivirus and anti-malware tools to scan and clean the affected endpoints.

    - Manually inspect systems if needed for any remaining traces of ransomware.
- Update all software and apply necessary patches to address vulnerabilities exploited by the attackers.
    - Ensure the latest security updates are installed on all systems.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.
- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore encrypted files from backups, ensuring the backups are clean and free from ransomware.
    - Verify the integrity and functionality of restored files and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of reinfection.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the ransomware entered the network.
    - Review logs, endpoint data, and network traffic to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial infection to containment and eradication.

Preventive Measures:

- Implement stronger email filtering and user training to reduce the risk of phishing attacks.
- Enhance network segmentation and access controls to minimize the impact of future attacks.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.

    - Lessons learned and recommendations for improving security posture.
- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** Ryuk Ransomware
- **Entry Point:** Likely phishing email with malicious attachment or link
- **Affected Systems:** 15 workstations, 2 file servers
- **Detection:** EDR alerts and user reports
- **Containment:** Network isolation, blocking of malicious IPs, URLs, and file-sharing protocols
- **Eradication:** Malware removal, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Temporary data unavailability, potential financial and reputational damage
- **Mitigation:** Enhanced email filtering, user training, network segmentation, incident response testing

SCENARIO 2: DATA EXFILTRATION VIA PHISHING ATTACK

On a busy Wednesday afternoon, you receive alerts from the SIEM system indicating multiple login attempts from unusual IP addresses on the organization's email server. Concurrently, several employees report receiving phishing emails.

Incident Response Steps

Step 1: Identification

Alerts:

- SIEM alerts for multiple failed and successful login attempts from foreign IP addresses.
- EDR alerts for unusual network traffic from internal systems to external IP addresses.
- Employees report receiving suspicious emails asking for login credentials.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the phishing attack.
- Identify the affected systems and users using logs from SIEM, email server logs, and EDR tools.
- Note: The phishing emails are identified as part of a known campaign targeting healthcare organizations.

System Logs from Infected Machine (Host: WORKSTATION-02)

1. SIEM Alert Logs:

2024-07-23 14:12:45 [ALERT] Multiple failed login attempts detected - User: Iffah, IP: 203.0.113.45
2024-07-23 14:13:10 [ALERT] Successful login from unusual IP address - User: Iffah, IP: 203.0.113.45
2024-07-23 14:14:30 [ALERT] Large data transfer detected to external IP - User: Iffah, Destination IP: 198.51.100.50

2. Email Server Logs:

2024-07-23 14:11:55 [Event ID 1000] Email received from suspicious sender - From: attacker@example.com, To: Iffah@example.com
2024-07-23 14:12:05 [Event ID 1001] Email opened - User: Iffah, Subject: "Urgent: Password Reset Required"
2024-07-23 14:12:10 [Event ID 1002] Link clicked in email - User: Iffah, URL: http://malicious-link.com

3. Firewall Logs:

2024-07-23 14:13:35 [ALERT] Outbound connection attempt detected - Destination IP: 198.51.100.50, Port: 443
2024-07-23 14:14:00 [ALERT] Large data transfer detected - Source: WORKSTATION-02, Destination IP: 198.51.100.50

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the affected machine (WORKSTATION-02) from the network to prevent further data exfiltration.
  - Use network segmentation to isolate critical systems from those that are potentially compromised.
  - Disable any remote access (e.g., RDP, VPN) to the affected machines.
- **Blocking:**
  - Block known malicious IP addresses, domains, and URLs associated with the phishing campaign.
  - Implement temporary blocks on email attachments and URLs until the investigation is complete.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, and legal teams, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., avoid opening suspicious emails).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the SIEM alerts and email server logs to identify compromised accounts and infected systems (e.g., WORKSTATION-02).
   - Verify the extent of the infection using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the infected machines from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the devices.

     ```
     # Example command to disable network interface on Windows
     netsh interface set interface "Ethernet" admin=disable
     ```

   - **Endpoint Isolation:**

        - Use EDR or remote management tools to isolate the infected endpoints.

```
# Example using an EDR platform command
edr isolate-endpoint --hostname WORKSTATION-02
```

Blocking Steps:

1. **Block Malicious IP Addresses:**
    - Use firewall rules to block outbound connections to known malicious IP addresses.

```
# Example command to block an IP address using Windows Firewall
netsh advfirewall firewall add rule name="Block Phishing IP" dir=out
action=block remoteip=198.51.100.50
```

2. **Block Malicious Domains and URLs:**
    - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the phishing campaign.

```
# Example using a DNS filtering solution
dns-filter add --domain "malicious-link.com" --action block
```

3. **Restrict Email Attachments:**
    - Disable or limit access to email attachments and links until the investigation is complete.

```
# Example command to disable email attachments in Office 365
Set-TransportRule -Name "Block Attachments" -AttachmentAction Block -
AttachmentType "all"
```

4. **Monitor and Verify:**
    - Continuously monitor network traffic and logs to ensure no further malicious activities.
    - Verify that all blocks and isolation measures are effectively preventing further data exfiltration.

Step 3: Eradication

Eradication Actions:

- Remove the phishing emails from all affected mailboxes.
    - Use email filtering tools to scan and remove any remaining malicious emails.

```
# Example command to remove phishing emails in Office 365
Search-Mailbox -SearchQuery "From:attacker@example.com" -DeleteContent
```

- Remove any malware or malicious scripts identified on the infected systems.
    - Use antivirus and anti-malware tools to scan and clean the affected endpoints.
    - Manually inspect systems if needed for any remaining traces of malware.
- Update all software and apply necessary patches to address vulnerabilities exploited by the attackers.
    - Ensure the latest security updates are installed on all systems.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.
- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore any exfiltrated data from backups, ensuring the backups are clean and free from malware.
    - Verify the integrity and functionality of restored data and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of reinfection.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the phishing attack succeeded.
    - Review logs, email server data, and network traffic to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial infection to containment and eradication.

Preventive Measures:

- Implement stronger email filtering and user training to reduce the risk of phishing attacks.
- Enhance network segmentation and access controls to minimize the impact of future attacks.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.
    - Lessons learned and recommendations for improving security posture.
- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** Data Exfiltration via Phishing
- **Entry Point:** Phishing email with malicious link
- **Affected Systems:** 10 user accounts, 1 workstation (WORKSTATION-02)
- **Detection:** SIEM alerts and user reports
- **Containment:** Network isolation, blocking of malicious IPs, URLs, and email attachments
- **Eradication:** Removal of phishing emails, malware cleaning, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Potential data breach, temporary data unavailability, reputational damage
- **Mitigation:** Enhanced email filtering, user training, network segmentation, incident response testing

SCENARIO 3: SQL INJECTION ATTACK ON A WEB APPLICATION

Late on a Friday evening, you receive alerts from the web application firewall (WAF) indicating multiple SQL injection attempts targeting the company's customer database.

Incident Response Steps

Step 1: Identification

Alerts:

- WAF alerts for SQL injection patterns in HTTP requests.
- Database server logs showing unusual query patterns and high CPU usage.
- SIEM alerts for data exfiltration attempts.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the SQL injection attack.
- Identify the affected systems and databases using logs from the WAF, database servers, and SIEM tools.
- Note: The SQL injection attack appears to be targeting sensitive customer information stored in the database.

System Logs from Infected Machine (Database Server: DB-SERVER-01)

1. WAF Alert Logs:

2024-07-23 22:45:12 [ALERT] SQL injection pattern detected in HTTP request - URL: /product?id=1; DROP TABLE users; --
2024-07-23 22:45:25 [ALERT] SQL injection pattern detected in HTTP request - URL: /search?query=' OR 1=1 --
2024-07-23 22:45:40 [ALERT] Multiple SQL injection attempts detected - Source IP: 192.0.2.45

2. Database Server Logs:

2024-07-23 22:44:58 [Event ID 18456] Login failed for user 'sa' - IP: 192.0.2.45
2024-07-23 22:45:10 [Event ID 17806] Error: 18456, Severity: 14, State: 8.
2024-07-23 22:45:22 [Event ID 4690] High CPU usage detected - Process: sqlservr.exe
2024-07-23 22:45:30 [Event ID 4691] Unusual query execution pattern - Query: SELECT * FROM users WHERE 1=1

3. SIEM Alert Logs:

2024-07-23 22:45:35 [ALERT] Data exfiltration attempt detected - Source: DB-SERVER-01, Destination IP: 198.51.100.50, Port: 443

2024-07-23 22:45:50 [ALERT] Unusual network traffic detected - Source: DB-SERVER-01, Destination IP: 198.51.100.50

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the affected database server (DB-SERVER-01) from the network to prevent further data exfiltration.
  - Use network segmentation to isolate the web application and database servers from other critical systems.
  - Disable any remote access (e.g., SSH, RDP) to the affected servers.
- **Blocking:**
  - Block the known malicious IP addresses, domains, and URLs associated with the SQL injection attack.
  - Implement temporary blocks on suspicious HTTP requests containing SQL injection patterns.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, and legal teams, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., avoiding use of the affected web application).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the WAF alerts and database server logs to identify compromised accounts and infected systems (e.g., DB-SERVER-01).
   - Verify the extent of the infection using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the infected machines from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the devices.

     ```
     # Example command to disable network interface on Windows
     netsh interface set interface "Ethernet" admin=disable
     ```

   - **Endpoint Isolation:**
     - Use EDR or remote management tools to isolate the infected endpoints.

```
# Example using an EDR platform command
edr isolate-endpoint --hostname DB-SERVER-01
```

Blocking Steps:

1. **Block Malicious IP Addresses:**
   - Use firewall rules to block outbound connections to known malicious IP addresses.

```
# Example command to block an IP address using Windows Firewall
netsh advfirewall firewall add rule name="Block SQL Injection IP" dir=out
action=block remoteip=198.51.100.50
```

2. **Block Malicious Domains and URLs:**
   - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the SQL injection attack.

```
# Example using a DNS filtering solution
dns-filter add --domain "malicious-domain.com" --action block
```

3. **Restrict Suspicious HTTP Requests:**
   - Configure the WAF to block or alert on HTTP requests containing SQL injection patterns.

```
# Example configuration to block SQL injection patterns in ModSecurity WAF
SecRule ARGS "@rx
(?:union.*select.*\b(?:from|into)\b|select.*\b(?:from|into)\b.*\bunion\b)" \
"id:12345,phase:2,deny,status:403,log,msg:'SQL Injection Attempt'"
```

4. **Monitor and Verify:**
   - Continuously monitor network traffic and logs to ensure no further malicious activities.
   - Verify that all blocks and isolation measures are effectively preventing further data exfiltration.

Step 3: Eradication

Eradication Actions:

- Remove the SQL injection vulnerabilities from the web application code.
  - Review and sanitize all user inputs to prevent SQL injection.
  - Use prepared statements and parameterized queries in the application code.
- Remove any malware or malicious scripts identified on the infected systems.
  - Use antivirus and anti-malware tools to scan and clean the affected endpoints.
  - Manually inspect systems if needed for any remaining traces of malware.

- Update all software and apply necessary patches to address vulnerabilities exploited by the attackers.
    - Ensure the latest security updates are installed on all systems.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.
- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore any corrupted or exfiltrated data from backups, ensuring the backups are clean and free from malware.
    - Verify the integrity and functionality of restored data and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of reinfection.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the SQL injection attack succeeded.
    - Review logs, web application code, and database server data to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial infection to containment and eradication.

Preventive Measures:

- Implement stronger input validation and output encoding to prevent SQL injection attacks.
- Enhance network segmentation and access controls to minimize the impact of future attacks.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.
    - Lessons learned and recommendations for improving security posture.

- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** SQL Injection Attack
- **Entry Point:** Vulnerable web application
- **Affected Systems:** 1 database server (DB-SERVER-01), web application
- **Detection:** WAF alerts, database server logs, and SIEM alerts
- **Containment:** Network isolation, blocking of malicious IPs, URLs, and suspicious HTTP requests
- **Eradication:** Code review and sanitization, malware removal, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Potential data breach, temporary data unavailability, reputational damage
- **Mitigation:** Enhanced input validation, user training, network segmentation, incident response testing

SCENARIO 4: RANSOMWARE ATTACK ON INTERNAL NETWORK

Early on a Monday morning, employees report that they are unable to access files and are seeing ransom notes on their screens. The ransom note demands payment in cryptocurrency to decrypt the files.

Incident Response Steps

Step 1: Identification

Alerts:

- SIEM alerts for unusual file encryption activities across multiple workstations.
- EDR alerts indicating ransomware signatures on endpoints.
- Employees report inability to access files and seeing ransom notes.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the ransomware attack.
- Identify the affected systems and the scope of the attack using logs from SIEM, EDR tools, and user reports.
- Note: The ransomware has encrypted critical files across several departments.

System Logs from Infected Machine (Workstation: WORKSTATION-05)

1. SIEM Alert Logs:

2024-07-22 08:01:12 [ALERT] Unusual file encryption detected - Host: WORKSTATION-05
2024-07-22 08:01:20 [ALERT] High number of file modifications - Host: WORKSTATION-05
2024-07-22 08:01:35 [ALERT] Suspicious process execution - Process: encrypt.exe

2. EDR Alert Logs:

2024-07-22 08:00:50 [ALERT] Ransomware signature detected - File: C:\Users\Iffah\AppData\Local\Temp\encrypt.exe
2024-07-22 08:01:05 [ALERT] Process execution - encrypt.exe started by user Iffah
2024-07-22 08:01:30 [ALERT] File encryption activity - C:\Users\Iffah\Documents*.docx

3. User Reports:

2024-07-22 08:05:00 [REPORT] Unable to access files, ransom note displayed - User: Eliff, Department: Finance
2024-07-22 08:05:10 [REPORT] Ransom note text: "Your files have been encrypted. Pay 5 BTC to the following address to get the decryption key."

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the infected machines (e.g., WORKSTATION-05) from the network to prevent further spread of the ransomware.
  - Use network segmentation to isolate critical systems from those that are potentially compromised.
  - Disable any remote access (e.g., RDP, VPN) to the affected machines.
- **Blocking:**
  - Block known malicious IP addresses, domains, and URLs associated with the ransomware command and control (C2) servers.
  - Implement temporary blocks on suspicious network traffic until the investigation is complete.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, and legal teams, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., avoid turning off infected machines).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the SIEM and EDR alerts to identify compromised accounts and infected systems (e.g., WORKSTATION-05).
   - Verify the extent of the infection using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the infected machines from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the devices.

     ```
     # Example command to disable network interface on Windows
     netsh interface set interface "Ethernet" admin=disable
     ```

   - **Endpoint Isolation:**
     - Use EDR or remote management tools to isolate the infected endpoints.

     ```
     # Example using an EDR platform command
     edr isolate-endpoint --hostname WORKSTATION-05
     ```

Blocking Steps:

1. **Block Malicious IP Addresses:**
    - Use firewall rules to block outbound connections to known malicious IP addresses associated with ransomware C2 servers.

    # Example command to block an IP address using Windows Firewall
    netsh advfirewall firewall add rule name="Block Ransomware C2 IP" dir=out action=block remoteip=203.0.113.10

2. **Block Malicious Domains and URLs:**
    - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the ransomware attack.

    # Example using a DNS filtering solution
    dns-filter add --domain "malicious-domain.com" --action block

3. **Restrict Suspicious Network Traffic:**
    - Configure firewalls and intrusion prevention systems (IPS) to block suspicious network traffic patterns.

    # Example using a firewall configuration
    ufw deny out from any to 203.0.113.0/24

4. **Monitor and Verify:**
    - Continuously monitor network traffic and logs to ensure no further malicious activities.
    - Verify that all blocks and isolation measures are effectively preventing further spread of the ransomware.

Step 3: Eradication

Eradication Actions:

- Remove the ransomware from infected systems.
    - Use antivirus and anti-malware tools to scan and clean the affected endpoints.
    - Manually inspect systems if needed for any remaining traces of ransomware.
- Update all software and apply necessary patches to address vulnerabilities exploited by the attackers.
    - Ensure the latest security updates are installed on all systems.
- Conduct a thorough investigation to identify and close any security gaps that allowed the ransomware to infiltrate the network.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.
- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore encrypted data from backups, ensuring the backups are clean and free from malware.
    - Verify the integrity and functionality of restored data and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of reinfection.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the ransomware attack succeeded.
    - Review logs, ransomware samples, and network traffic to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial infection to containment and eradication.

Preventive Measures:

- Implement stronger email filtering and user training to reduce the risk of phishing and ransomware attacks.
- Enhance network segmentation and access controls to minimize the impact of future attacks.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.
    - Lessons learned and recommendations for improving security posture.
- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** Ransomware Attack
- **Entry Point:** User clicked on malicious link in a phishing email
- **Affected Systems:** Multiple workstations (e.g., WORKSTATION-05)
- **Detection:** SIEM alerts, EDR alerts, and user reports
- **Containment:** Network isolation, blocking of malicious IPs, URLs, and suspicious network traffic
- **Eradication:** Ransomware removal, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Data encryption, temporary data unavailability, potential financial loss, reputational damage
- **Mitigation:** Enhanced email filtering, user training, network segmentation, incident response testing

SCENARIO 5: ADVANCED PERSISTENT THREAT (APT) ATTACK

Mid-week, you receive alerts from your threat detection systems indicating unusual activity on several internal servers. Further investigation reveals that an advanced persistent threat (APT) group has infiltrated your network and is conducting reconnaissance and data exfiltration.

Incident Response Steps

Step 1: Identification

Alerts:

- SIEM alerts for unusual login attempts and privilege escalation.
- EDR alerts indicating the presence of advanced malware.
- Network traffic analysis showing data exfiltration to an unknown external IP.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the APT attack.
- Identify the affected systems and the scope of the attack using logs from SIEM, EDR tools, and network traffic analysis.
- Note: The APT group is targeting sensitive financial data stored on internal servers.

System Logs from Infected Machine (Internal Server: SERVER-02)

1. SIEM Alert Logs:

2024-07-20 11:05:12 [ALERT] Unusual login attempts detected - Host: SERVER-02, User: admin
2024-07-20 11:05:20 [ALERT] Privilege escalation detected - Process: cmd.exe
2024-07-20 11:05:35 [ALERT] Unauthorized access attempt - File: /etc/passwd

2. EDR Alert Logs:

2024-07-20 11:04:50 [ALERT] Advanced malware detected - File: C:\Windows\Temp\exploit.dll
2024-07-20 11:05:05 [ALERT] Suspicious process execution - Process: powershell.exe
2024-07-20 11:05:30 [ALERT] Data exfiltration activity - File: C:\SensitiveData*.csv

3. Network Traffic Analysis:

2024-07-20 11:05:35 [ALERT] Unusual outbound traffic detected - Source: SERVER-02, Destination IP: 198.51.100.20, Port: 443
2024-07-20 11:05:50 [ALERT] Data transfer to external IP - Source: SERVER-02, Destination IP: 198.51.100.20

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the infected servers (e.g., SERVER-02) from the network to prevent further data exfiltration.
  - Use network segmentation to isolate critical systems from those that are potentially compromised.
  - Disable any remote access (e.g., SSH, RDP) to the affected servers.
- **Blocking:**
  - Block known malicious IP addresses, domains, and URLs associated with the APT group's command and control (C2) servers.
  - Implement temporary blocks on suspicious network traffic until the investigation is complete.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, and legal teams, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., avoid accessing sensitive systems).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the SIEM and EDR alerts to identify compromised accounts and infected systems (e.g., SERVER-02).
   - Verify the extent of the infection using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the infected machines from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the devices.

     ```
     # Example command to disable network interface on Windows
     netsh interface set interface "Ethernet" admin=disable
     ```

   - **Endpoint Isolation:**
     - Use EDR or remote management tools to isolate the infected endpoints.

     ```
     # Example using an EDR platform command
     edr isolate-endpoint --hostname SERVER-02
     ```

Blocking Steps:

1. **Block Malicious IP Addresses:**
    - Use firewall rules to block outbound connections to known malicious IP addresses associated with APT C2 servers.

    # Example command to block an IP address using Windows Firewall
    netsh advfirewall firewall add rule name="Block APT C2 IP" dir=out action=block remoteip=198.51.100.20

2. **Block Malicious Domains and URLs:**
    - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the APT group.

    # Example using a DNS filtering solution
    dns-filter add --domain "malicious-domain.com" --action block

3. **Restrict Suspicious Network Traffic:**
    - Configure firewalls and intrusion prevention systems (IPS) to block suspicious network traffic patterns.

    # Example using a firewall configuration
    ufw deny out from any to 198.51.100.0/24

4. **Monitor and Verify:**
    - Continuously monitor network traffic and logs to ensure no further malicious activities.
    - Verify that all blocks and isolation measures are effectively preventing further data exfiltration.

Step 3: Eradication

Eradication Actions:

- Remove the advanced malware from infected systems.
    - Use antivirus and anti-malware tools to scan and clean the affected endpoints.
    - Manually inspect systems if needed for any remaining traces of malware.
- Update all software and apply necessary patches to address vulnerabilities exploited by the attackers.
    - Ensure the latest security updates are installed on all systems.
- Conduct a thorough investigation to identify and close any security gaps that allowed the APT group to infiltrate the network.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.

- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore any corrupted or exfiltrated data from backups, ensuring the backups are clean and free from malware.
    - Verify the integrity and functionality of restored data and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of reinfection.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the APT attack succeeded.
    - Review logs, malware samples, and network traffic to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial infection to containment and eradication.

Preventive Measures:

- Implement stronger network monitoring and threat detection to identify APT activities early.
- Enhance network segmentation and access controls to minimize the impact of future attacks.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.
    - Lessons learned and recommendations for improving security posture.
- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** Advanced Persistent Threat (APT) Attack

- **Entry Point:** Exploited vulnerabilities in internal servers
- **Affected Systems:** Multiple internal servers (e.g., SERVER-02)
- **Detection:** SIEM alerts, EDR alerts, and network traffic analysis
- **Containment:** Network isolation, blocking of malicious IPs, URLs, and suspicious network traffic
- **Eradication:** Malware removal, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Data exfiltration, temporary data unavailability, potential financial loss, reputational damage
- **Mitigation:** Enhanced network monitoring, user training, network segmentation, incident response testing

Incident Response Simulation

Scenario: Insider Threat and Data Breach

Background: One afternoon, unusual activity is detected on a database server containing sensitive patient information. Further investigation reveals that an insider has been accessing and exfiltrating sensitive data.

Incident Response Steps

Step 1: Identification

Alerts:

- SIEM alerts for unusual access patterns and large data transfers from the database server.
- DLP (Data Loss Prevention) alerts indicating potential data exfiltration.
- User behaviour analytics (UBA) showing anomalous activity by a specific employee.

Initial Actions:

- Verify the alerts and analyse the indicators of compromise (IoCs) associated with the data breach.
- Identify the affected systems and the scope of the breach using logs from SIEM, DLP tools, and user behaviour analytics.
- Note: The insider is accessing patient data and exfiltrating it to an external server.

System Logs from Infected Machine (Database Server: DB-SERVER-01)

1. SIEM Alert Logs:

2024-07-21 15:30:12 [ALERT] Unusual access patterns detected - Host: DB-SERVER-01, User: insider
2024-07-21 15:30:20 [ALERT] Large data transfer detected - Host: DB-SERVER-01, Destination IP: 203.0.113.10
2024-07-21 15:30:35 [ALERT] Suspicious database queries - User: insider

2. DLP Alert Logs:

2024-07-21 15:29:50 [ALERT] Data exfiltration attempt detected - File: /patient_records/*.csv
2024-07-21 15:30:05 [ALERT] Data transfer to external IP - Source: DB-SERVER-01, Destination IP: 203.0.113.10
2024-07-21 15:30:30 [ALERT] Unauthorized data access - User: insider

3. User Behaviour Analytics:

2024-07-21 15:28:35 [ALERT] Anomalous login time detected - User: insider
2024-07-21 15:29:00 [ALERT] High volume of data access - User: insider
2024-07-21 15:29:25 [ALERT] Accessing sensitive data outside of normal hours - User: insider

Step 2: Containment

Immediate Containment Actions:

- **Isolation:**
  - Immediately isolate the database server (e.g., DB-SERVER-01) from the network to prevent further data exfiltration.
  - Temporarily disable the compromised user account (e.g., insider) to stop unauthorized access.
  - Use network segmentation to isolate critical systems from those that are potentially compromised.
- **Blocking:**
  - Block known malicious IP addresses and domains associated with the data exfiltration.
  - Implement temporary blocks on suspicious network traffic until the investigation is complete.
  - Utilize firewalls and network access control (NAC) to enforce these blocks.

Communication:

- Inform relevant stakeholders, including IT, management, legal teams, and data privacy officers, about the ongoing incident.
- Provide clear instructions to employees on what actions to take (e.g., avoid accessing the compromised database server).

Isolation Steps:

1. **Identify Infected Machines:**
   - Use the SIEM and DLP alerts to identify compromised accounts and infected systems (e.g., DB-SERVER-01).
   - Verify the extent of the breach using SIEM logs and network traffic analysis.
2. **Isolate the Infected Machines:**
   - **Network Isolation:**
     - Disconnect the database server from the network.
     - If physical disconnection is not feasible, use network access control (NAC) to quarantine the device.

     ```
     # Example command to disable network interface on Linux
     ifconfig eth0 down
     ```

   - **Account Isolation:**

- Disable the compromised user account.

```
# Example using a Linux command to disable a user account
usermod -L insider
```

Blocking Steps:

1. **Block Malicious IP Addresses:**
   - Use firewall rules to block outbound connections to known malicious IP addresses associated with the data exfiltration.

```
# Example command to block an IP address using Windows Firewall
netsh advfirewall firewall add rule name="Block Exfil IP" dir=out action=block
remoteip=203.0.113.10
```

2. **Block Malicious Domains and URLs:**
   - Update DNS filtering or web proxy rules to block access to malicious domains and URLs associated with the exfiltration.

```
# Example using a DNS filtering solution
dns-filter add --domain "malicious-domain.com" --action block
```

3. **Restrict Suspicious Network Traffic:**
   - Configure firewalls and intrusion prevention systems (IPS) to block suspicious network traffic patterns.

```
# Example using a firewall configuration
ufw deny out from any to 203.0.113.0/24
```

4. **Monitor and Verify:**
   - Continuously monitor network traffic and logs to ensure no further malicious activities.
   - Verify that all blocks and isolation measures are effectively preventing further data exfiltration.

Step 3: Eradication

Eradication Actions:

- Remove any malicious software or scripts used by the insider from infected systems.
  - Use antivirus and anti-malware tools to scan and clean the affected endpoints.
  - Manually inspect systems if needed for any remaining traces of malicious activity.
- Update all software and apply necessary patches to address vulnerabilities exploited by the insider.
  - Ensure the latest security updates are installed on all systems.

- Conduct a thorough investigation to identify and close any security gaps that allowed the insider to exploit the network.

Credential Reset:

- Reset passwords for compromised accounts and ensure multi-factor authentication (MFA) is enforced.
- Monitor for any suspicious account activities post-incident.

Step 4: Recovery

Recovery Actions:

- Restore any corrupted or exfiltrated data from backups, ensuring the backups are clean and free from malware.
    - Verify the integrity and functionality of restored data and systems.
- Conduct a thorough inspection of the network to ensure no hidden malware or backdoors remain.
- Gradually bring systems back online, monitoring closely for any signs of further malicious activity.

Step 5: Lessons Learned

Post-Incident Analysis:

- Conduct a detailed root cause analysis (RCA) to understand how the insider threat succeeded.
    - Review logs, user activities, and network traffic to trace the attack vector.
- Document findings and create a timeline of the attack, detailing each stage from initial access to containment and eradication.

Preventive Measures:

- Implement stronger user behaviour analytics and monitoring to detect insider threats early.
- Enhance network segmentation and access controls to minimize the impact of future insider threats.
- Regularly test incident response plans and conduct simulations to improve readiness.

Reporting:

- Prepare a comprehensive incident report detailing:
    - The nature and scope of the incident.
    - Steps taken during the incident response process.
    - Lessons learned and recommendations for improving security posture.
- Share the report with relevant stakeholders, including IT, management, and regulatory bodies if required.

Full Analysis and Report

Incident Summary:

- **Attack Type:** Insider Threat and Data Breach
- **Entry Point:** Authorized access by a trusted employee
- **Affected Systems:** Database server (e.g., DB-SERVER-01)
- **Detection:** SIEM alerts, DLP alerts, and user behaviour analytics
- **Containment:** Network isolation, blocking of malicious IPs, and suspicious network traffic
- **Eradication:** Malicious software removal, software updates, and patching
- **Recovery:** Data restoration from clean backups, system integrity checks
- **Impact:** Data exfiltration, potential privacy breaches, reputational damage
- **Mitigation:** Enhanced user behaviour analytics, network segmentation, incident response testing